decrypting the session key at the intermediary;

decrypting, at the intermediary, the encrypted data using the session key; and

inspecting the data in route between the internal and external clients.

20. (Unchanged) In a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints, computer-readable media at one of the endpoints and at the intermediary storing computer-executable instructions for:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption.

REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-20 are pending.

35 U.S.C. §112

The Examiner has withdrawn the 35 U.S.C. §112 rejection of claims 3, 7, 8-11 of the previous office action.

35 U.S.C. §101

The Examiner has withdrawn the 35 U.S.C. §101 rejection of claims 12-18 of the previous office action.

35 U.S.C. §102

Claims 1 and 4 remain rejected under 35 U.S.C. §102 as being anticipated by U.S. Patent 5,835,726 to Shwed et al (Shwed). Applicants respectfully traverse the rejection.

The invention concerns a network architecture in which two endpoints communicate via a virtual private network (VPN) on an otherwise public network, such as the Internet, and an intermediary is permitted to inspect the data communication in a secure and trusted manner.

In one implementation, the network architecture has an external client and an internal client that exchange encrypted data over a network. The internal client is coupled to the network via a network access point, such as a firewall/proxy server. All three participants have their own pair of public/private keys. An independent key server holds the public keys for all three participants.

The external and internal clients establish a virtual private network by negotiating a session key used to encrypt data being exchanged between them. Initially, only the clients know the session key, and not the firewall. To grant the firewall trusted access to the data stream on the VPN, the internal client securely transfers the session key to the firewall. The internal client requests and receives the firewall's public key from the key server and encrypts the session key using the firewall's public key. The internal client then signs the encrypted key by encrypting it using the internal client's private key.

The firewall authenticates the signature by decrypting the message using the internal client's public key (obtained from the key server or directly from the internal computer). The firewall then decrypts the session key using its own private key. If the dual decryption yields a valid key, the firewall is assured that the session key was sent by the internal client and was not subsequently altered or tampered with in route.

Once the session key is transferred, the firewall is able to decrypt the data stream on the VPN. The firewall can now un-intrusively inspect the data stream in a manner that is transparent to the external and internal clients. The claims capture this architecture and new technology.

Fig. 2 of the present application is representative of the invention and is reproduced below.

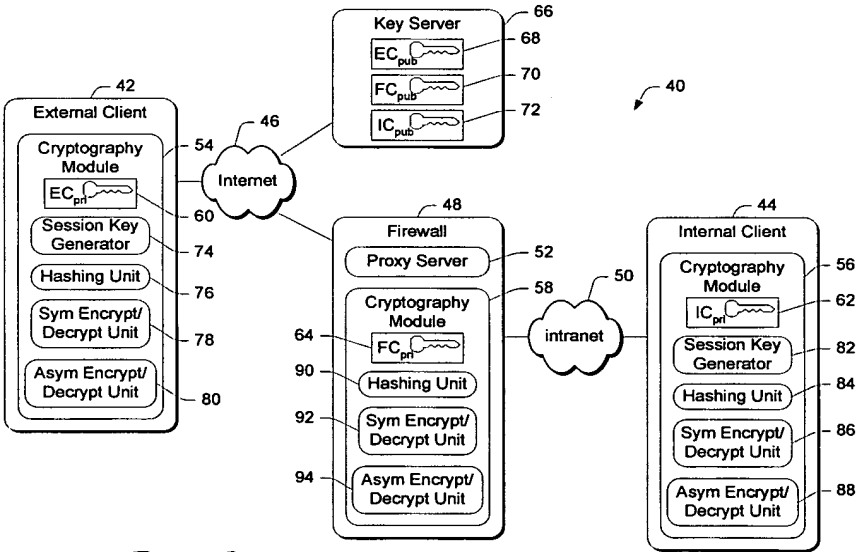

Fig. 2

Claim 1 for example recites a "method for inspecting an encrypted data stream being transferred over a network between two endpoints, the data stream being encrypted using a session key known to both endpoints, the method comprising:

securely transferring the session key from one of the endpoints to an intermediary having access to the encrypted data stream;

decrypting the encrypted data stream at the intermediary using the session key; and

inspecting the data stream following decryption."

The method of claim 1 provides for an establishment of a virtual private network (VPN) between two computers (endpoints) where the computers (endpoints) engage in key negotiation process to negotiate a session key (see specification page 9, lines 11-13). With the session key, the endpoints (internal and external clients) are able to encrypt messages and begin an encrypted communication session directly with one another (see specification page 9, lines 11-17, Fig. 2). Once the session key is created, one of the endpoints is able to securely share the key with an intermediary to permit trusted inspection. All three participants have their own pair of public/private keys (see specification page 7, lines 11-17).

The method of claim 1 is not disclosed by Shwed. Shwed shows host 1 and host 2 computers (also referred to by the Examiner as endpoints) connected to respective private networks. Host 1 and Host 2 are secured through respective firewalls. The firewalls connect to one another by way of a public network. See Shwed, col 14, lines 19-39, Fig. 16. Host 1 and Host 2 do not directly communicate with one another.

Fig. 16 of Shwed is redrawn below.

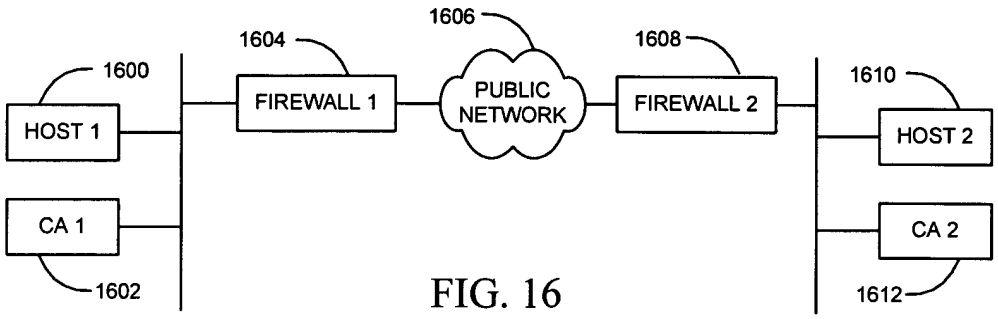

FIG. 16

Shwed does not teach or disclose that Host1 and Host2, one of which is considered an endpoint in Shwed, as knowing a session key. An element of the claims as recited in claim 1 is "a session key known to both endpoints." The Examiner has pointed to teachings in Shwed that show a session key that is known by a firewall or an outside client. In Shwed a session key is generated by the non-initiator firewall also called the destination and is sent encrypted to the initiator firewall (Shwed at col. 15, lines 33-35). Shwed does not teach or disclose that either Host 1 or Host 2 would know the session key, in view of the fact that Host1 or Host 2 do not decrypt or encrypt data. As discussed Shwed makes particular mention that communication to and from Host 1 and Host 2 are never encrypted, and does not teach or disclose that either Host 1 or Host 2 would know a session key. Either Host 1 or Host 2 is viewed as an endpoint the teaching of Shwed, however, in any configuration taught by Shwed neither Host 1 nor Host 2 will know a session key.

The Examiner argues that "Shwed desires that the communications between Host 1 and Host 2 be secured" referring to Shwed at col. 14, lines 40-41. However, this security is only performed through firewall 1 and firewall 2. In other words, secured communication disclosed or taught by Shwed is from firewall to firewall, or in other cases a client (host) to a firewall. "As stated previously,

only the communication between firewall1 and firewall2 are actually encrypted." (Shwed at col. 15 lines 31-32). "The communications between host1 and firewall1 and between host2 and firewall2 are not encrypted." (Shwed at col. 15 lines 8-10).

Shwed does not teach or disclose that Host 1 and Host 2, one of which is always an endpoint, to transfer an encrypted data stream between another or transfer an encrypted data stream to a firewall. An element of the claims as recited in claim 1 is "an encrypted data stream being transferred over a network between two endpoints." Shwed discloses a public network 1606 in Fig. 1606. The Examiner argues that firewall 1 and firewall 2 may be treated as intermediaries and/or as sources (i.e., endpoints). The Examiner states in the office action "Firewall1 is a source of transmitting encrypted packet[s] to intermediary firewall2, while it is also an intermediary point for inspecting packets received from host2." In this arrangement, firewall 1 is an endpoint and host 2 is the other endpoint, and firewall 2 is an intermediary. An encrypted data stream never is transferred over the network 1606 between the two endpoints (i.e., firewall 1 and host 2). Since at least one host in Shwed is always considered an endpoint and a host never encrypts data, Shwed fails to teach or disclose "an encrypted data stream being transferred over a network between two endpoints."

For these reasons and those cited in the response to the previous office action, claim 1 is patentable over Shwed. Applicants respectfully request that the §102 rejection of claim 1 be withdrawn.

Dependent claim 4 is allowable by virtue of its dependency on base claim 1. For the reasons given above with respect to claim 1, the systems and methods recited in claim 4 are neither disclosed nor taught by Shwed. Applicants respectfully request that the §102 rejection of claim 4 be withdrawn.

35 U.S.C. §103

Claims 2, 3 and 5-20 are rejected under 35 U.S.C. §103 as being unpatentable over Shwed in view of Bruce Schneier, Applied Cryptography, Second Addition, 1996 (Schneier). Applicants respectfully traverse the rejection.

Claims 2 and 3 depend from claim 1 and hence incorporate the features of claim 1. As such claims 2 and 3 require "using a session key known to both endpoints."

Shwed does not suggest or teach a session key known to both endpoints. The session key in Shwed is known only by and between the intermediary firewalls not the endpoint computers host1 and host2. Host1 and host2 do not share a common session key nor are they involved in encryption with one another. The Examiner points out that one of the firewalls may be treated as an endpoint, in as much as the firewalls do know a session key. However, in configurations that are taught by Shwed, either host1 or host2 is considered an endpoint. Shwed does not does suggest or teach that either host1 or host2 as knowing a session key.

Schneier is cited for its teaching of known cryptosystems, in particular key exchange systems. Schneier provides no assistance as to the recited methodology of claims 2 and 3. Accordingly, a combination of Shwed and Schneier fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claims 2 and 3 be withdrawn.

Claim 5 defines "a method for inspecting an encrypted data stream being transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints ... passing the signed encrypted session key to the intermediary." As discussed, the

Shwed/Schneier combination does not suggest nor teach encrypted data streams that are transferred between two endpoints using a session key known to the two endpoints. The Shwed/Schneier combination does not suggest nor teach that a session key be passed from an endpoint to an intermediary. Therefore, even in view of Schneier, claim 5 is not obvious. Applicants respectfully request that the §103 rejection of claim 5 be withdrawn.

Dependent claim 6 is allowable by virtue of its dependency on base claim 5. Applicants respectfully request that the §103 rejection of claim 6 be withdrawn.

Amended claim 7 defines "in a network system having an internal client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients ... a method executed at the firewall comprising receiving an encrypted and signed session key from the internal client." As discussed, the Shwed/Schneier combination does not suggest nor teach that an internal client exchange encrypted data with an external client using a session key known to the internal and external clients. Applicants respectfully request that the §103 rejection of claim 7 be withdrawn.

Dependent claims 8, 9, 10, and 11 are allowable by virtue of their dependency on base claim 7. Applicants respectfully request that the §103 rejection of claims 8, 9, 10, and 11 be withdrawn.

Claim 12 defines "a network system comprising an internal client and an external client configured to communicate encrypted data over a network ..., the data being encrypted using a session key, the internal client being configured to securely transfer the session key to the intermediary."

In Shwed the internal client is either host1 or host 2. As discussed neither host1 nor host2 perform encrypted communication. Shwed makes particular mention that communication to and from host1 or host2 are not encrypted.

Schneier is cited for its teaching of known cryptosystems, in particular key exchange systems. Schneier provides no assistance as to the recited methodology of claim 12. Accordingly, a combination of Shwed and Schneier fails to teach or suggest the claimed methods. Applicants respectfully request that the §103 rejections of claim 12 be withdrawn.

Dependent claims 13, 14, and 15 are allowable by virtue of their dependency on base claim 12. Applicants respectfully request that the §103 rejection of claims 13, 14, and 15 be withdrawn.

Claim 16 defines "a software architecture for a network system having two endpoints that exchange encrypted data over a network and through an intermediary, the encrypted data being encrypted using a session key known to the endpoints comprising: endpoint-resident code stored on computer readable media and executable on a processor to encrypt the session key using a public key from a public/private key pair associated with the intermediary and to sign the encrypted session key with a digital signature, the endpoint-resident code being capable of sending the signed and encrypted session key to the intermediary; and intermediary-resident code stored on computer readable media and executable on the processor to authenticate the digital signature and decrypt the encrypted session key using a private key from the public/private key pair associated with the intermediary, the intermediary-resident code using the session key to decrypt the encrypted data as it is being exchanged between the two endpoints." As discussed, the Shwed/Schneier combination does not suggest nor teach that an

internal client exchange encrypted data with an external client using a session key known to the internal and external clients. The Shwed/Schneier combination fails to teach a session key known to the endpoints. The Shwed/Schneier combination fails to teach endpoint-resident code being capable of sending the signed and encrypted session key to the intermediary. The Shwed/Schneier combination further fails to teach intermediary-resident code using the session key to decrypt the encrypted data as it is being exchanged between the two endpoints. Applicants respectfully request that the §103 rejection of claim 16 be withdrawn.

Dependent claims 17 and 18 are allowable by virtue of their dependency on base claim 16. Applicants respectfully request that the §103 rejection of claims 17 and 18 be withdrawn.

Claim 19 defines "a network system having an internal client that exchanges encrypted data with an external client over a network and through a firewall intermediate of the internal and external clients, the encrypted data being encrypted using a session key known to the internal and external clients ... passing the signed and encrypted session key to the intermediary." As discussed, the Shwed/Schneier combination does not suggest nor teach that an internal client exchange encrypted data with an external client using a session key known to the internal and external clients. The Shwed/Schneier combination further fails to teach the session key being passed to the intermediary. Applicants respectfully request that the §103 rejection of claim 19 be withdrawn.

Claim 20 defines "a network system in which an encrypted data stream is transferred over a network between two endpoints and via an intermediary, the data stream being encrypted using a session key known to both endpoints ...securely transferring the session key from one of the endpoints to an

intermediary." As discussed, the Shwed/Schneier combination does not suggest nor teach that an internal client exchange encrypted data with an external client using a session key known to the internal and external clients. The Shwed/Schneier combination further fails to teach that the session key be transferred from one of the endpoints to an intermediary. Applicants respectfully request that the §103 rejection of claim 20 be withdrawn.

CONCLUSION

All pending claims 1-20 are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the subject application. If any issues remain that prevent issuance of this application, the Examiner is urged to contact the undersigned attorney before issuing a subsequent Action.

Respectfully Submitted,

Dated: 4/16/03

By: _____

Emmanuel A. Rivera
Reg. No. 45,760
(509) 324-9256 ext. 245